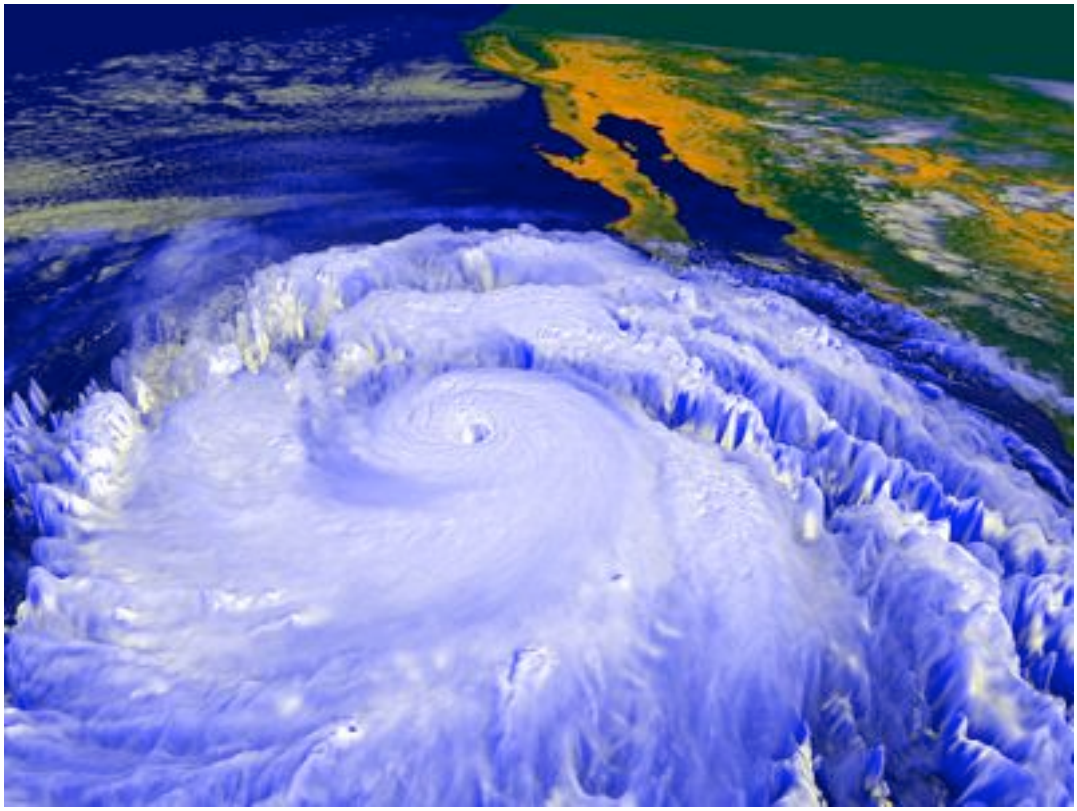
P E K K A N I K A N D E R

Helsinki Institute for Information Technology
and
Nomadic Lab, Ericsson Research, Finland

ON FUTURE INTERNET ARCHITECTURES: RETHINKING NAMING, TRUST, AND PRIMITIVES



Tammasaarenkatu 3, FI-02015 TKK, Finland • www.tml.hut.fi/~pnr/

Rethinking Naming, Trust, and Basic Primitives

Abstract

Naming and security are two major problems in the current Internet, needing fundamental rethinking. In this white paper, we describe our past and planned work related to the identifier / locator split in terms of the Host Identity Protocol (HIP), to trust and reputation in forms of Distributed Hash Tables (DHT) based trust and reputation networks, and more generally, to the fundamental networking primitives. Our work on the identifier / locator split has demonstrably already had impact on people's thinking at the IETF and other fora. We believe that our work on trust and reputation has potentially major impact in the 10–15 years perspective, and the planned work on networking primitives may have foundational impact on a slightly longer term perspective.

Past research and its impact

In the current Internet architecture, there are two major problems: incomplete naming and incompatible incentives. Incomplete naming, or the confounding of locators and identifiers in the form of IP addresses, is a major factor making mobility, multi-homing, delegation, and virtualisation unnecessarily difficult. Incompatible incentives, or an underlying trust model that assumes all networking parties having aligned and common communication goals, is the fundamental source for the main security problems, including unwanted traffic (SPAM and DDoS, among others), fraud, and farming of compromised hosts.

From 2000 to 2005, we focused in our research efforts on the naming problem, acting as a leader in pushing forward the Host Identity Protocol (HIP) ideas in the research and IETF communities [1]–[9]. In addition to the papers, the work has resulted in two open source implementations of HIP: HIP4BSD and HIPL. This work has had a clear effect on the way people think about the host / identity problem within the IETF and the larger community, including but not limited to the design of SHIM6, an **IETF standards** track protocol.

Before our focusing on mobility, security, and naming, and again more recently, we conducted research on trust, reputation, and delegation [10]–[13]. This work has created a better understanding of the economic forces and tensions underlying many current security problems (cf. [11]). In part, this work contributed to the forming of **security economics,** a new research area promoted by Dr. Ross Anderson and others.

Most recently, our early work on trust models and micro-economic analysis of protocols has led us to doubt the very primitives used in today's networked system, forcing us to reformulate the basic research questions. We envision a necessity of combining understanding from computational mechanism design, cryptographic protocols, graph theory and topology, and architectural understanding of mobile networking networking, leading to definition and experimentation of genuinely novel networking approaches.

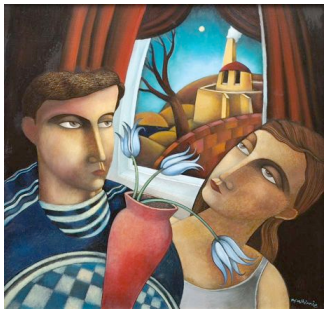
Planned research and a long-term vision

The current packet-based networking architecture can be seen as an extension of one inter-process communication mechanism: message passing. As we have seen, it works nicely as long as the senders' and receivers' incentives are aligned. However, as soon as there are enough of malicious senders who do not care about potential ill effects that they may cause to other users, or whose intention is outright denial of service, the vulnerability of the system becomes clear.

In a word, the current network has been designed to help the sender. The sender decides whom to send packets to; the receiver can ignore packets only once it has received and at least minimally processed them. In other words, in the current networks the sender knows the identity of the receiver and is able to send messages all the way through the network without the receiver's consent. This, together with zombie farms, creates a micro-economic situation where generating traffic is far cheaper than ignoring it, leading to the well known Denial of Service and SPAM problems. It is generally understood within Ericsson Research and HIIT that addressing these issues is of long term key importance.

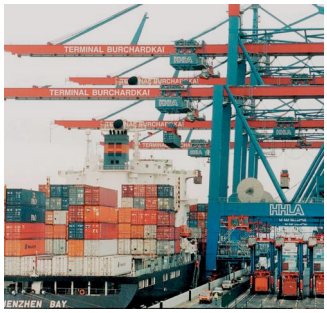
Based on the above, we strongly suspect that the current message-passing paradigm is closing to the end of its useful lifetime. In today's network, it is very clear how the incentive incompatibilities necessitate the introduction of increasingly more filtering and other controls. This is leading to the demise of the innovation period that was made possible by the generality and transparency of the original Internet design.

Looking at alternatives, the publish–subscribe paradigm looks like a promising one. Being a generalization of the tuple space or black board paradigm, e.g., as popularized by the Linda System[1] , publish–subscribe systems have many attractive properties that are relatively well understood in the context of operating systems, languages, and middleware; see e.g. [14][15]. However, much less attention has been paid on making some variant of the publish–subscribe scheme as the basic communication and networking primitive. Beside the well known benefits stemming from the multicast and loose coupling inherent to publish–subscribe, the very fact that in a publish–subscribe system the receiver has more control over what traffic to receive than in a traditional message-passing system seems to nicely contribute to solving the unwanted traffic problem without unnecessarily placing discriminatory power within the network.



Rendezvous

Routing



Forwarding

Technically, using publish–subscribe as the basic paradigm for communication networking requires us to partially rethink most of what we know about networking, including the basic primitives available to the upper layer protocols and applications, the mechanisms needed to implement bidirectional internetworking, the basic transport protocols, and the infrastructure services. At the primitives level, the traditional `send(receiver identity, data)` and `receive(sender identity, data)` primitives will be replaced with the `publish(publication identity, data)` and `subscribe(publication identity, data)` primitives. In internetworking, the traditionally confounded **rendezvous, routing,** and **forwarding** functions become necessarily separated. Transport protocols change since the underlying primitives change; however, the fundamental mechanisms for error and flow control are likely to stay relatively stable. Finally, the naming, security, and management infrastructures need to be reconsidered due to the changes in the underlying technology.

Funding and participation

Our work is funded partially by Ericsson Research Nomadic Lab and partially by Helsinki Institute for Information Technology (HIIT), a joint research institute of Helsinki University of Technology and University of Helsinki. In addition to direct institutional funding, HIIT and, to a lesser extend, Nomadic Lab, receive funding from Tekes, the Finnish governmental Funding Agency for Technology and Innovation, from European Union under various research programmes and project grants, and from other sources. This funding will include funding to a new planned joined activity with International Computer Science Institute (ICSI), the Finland-ICSI Center for Novel Internet Architectures.

I am, together with a small number of close colleagues both at Nomadic Lab and HIIT, working full time on the new research direction outlined above. Related to potential participation to FIND meetings, I have some personal limitations coupled with the family inconveniences caused by overseas traveling; you may want to consider other core members of the forthcoming Finland-ICSI Center in the occasions I cannot attend myself.

[1] Front page illustration: A 3D rendering of Linda the hurricane, http://rsd.gsfc.nasa.gov/rsd/images/Linda/linda_6_lg.jpg

Related web pages

InfraHIP project, http://www.infrahip.net/

Trustworthy Internet project, http://www.trustinet.org/

HIP4BSD implementation, http://www.hip4inter.net/

Selected publications

1. Robert Mozkowitz and Pekka Nikander, *Host Identity Protocol (HIP) Architecture*, RFC 4423, Internet Engineering Task Force, May 2006.
2. Teemu Koponen, Andrei Gurtov, Pekka Nikander, "Application mobility with Host Identity Protocol," in Proc. of *NDSS Wireless and Mobile Security Workshop*, San Diego, CA, USA, February 2005.
3. Pekka Nikander, Jari Arkko, and Börje Ohlman, Host Identity Indirection Infrastructure (Hi3)," in Proceedings of The *Second Swedish National Computer Networking Workshop 2004 (SNCNW2004)*, Karlstad University, Karlstad, Sweden, Nov 23-24, 2004.
4. Mikko Sarela, Pekka Nikander, "Applying Host Identity Protocol to Tactical Networks," in Proceedings of *Military Communications Conference (MILCOM2004)*, Monterey, CA, Oct 31-Nov 3, 2004.
5. Jukka Ylitalo, Jan Melen, Pekka Nikander, and Vesa Torvinen, "Re-thinking Security in IP based Micro-Mobility," in Proceedings of *7th Information Security Conference (ISC04)*, Palo Alto, CA, Sep 27-29, 2004.
6. Tuomas Aura, Pekka Nikander, and Gonzalo Camarillo, "Effects of Mobility and Multihoming on Transport-Layer Security," in Proceedings of *IEEE Symposium on Security and Privacy*, Berkeley/Oakland, California, May 9-12, 2004, IEEE Computer Society.
7. Jukka Ylitalo and Pekka Nikander, "BLIND: A Complete Identity Protection Framework for End-points", in *Security Protocols, Twelfth International Workshop*, Cambridge, 24-28 April, 2004.
8. Jukka Ylitalo, Pekka Nikander, "A new Name Space for End-Points: Implementing secure Mobility and Multi-homing across the two versions of IP," in Proceedings of the *Fifth European Wireless Conference, Mobile and Wireless Systems beyond 3G (EW2004)*, pp. 435-441, Barcelona, Spain, February 24-27, 2004.
9. Pekka Nikander, Jukka Ylitalo, and Jorma Wall, "Integrating Security, Mobility, and Multi-Homing in a HIP Way," in Proceedings of *Network and Distributed Systems Security Symposium (NDSS'03)*, February 6-7, 2003, San Diego, CA, pp. 87-99, Internet Society, February, 2003.
10. Pekka Nikander and Jari Arkko, "Delegation of Signalling Rights," in *Security Protocols, 10th International Workshop*, Cambridge, UK, April 16-19, 2002, LCNS 2845, pp. 203-212, Springer, 2003.
11. Jari Arkko and Pekka Nikander, "How to Authenticate Unknown Principals without Trusted Parties," in *Security Protocols, 10th International Workshop*, Cambridge, UK, April 16-19, 2002, LCNS 2845, pp. 5-16, Springer, 2003.
12. Pekka Nikander and Kristiina Karvonen, "Users and Trust in Cyberspace," in Christianson, Malcolm, Crispo and Roe (Eds.) *Security Protocols, 8th International Workshop, Cambridge*, UK, April 3-5, 2000; revised papers, LNCS 2133, pp. 24-35, Springer 2001.
13. Pekka Nikander, *An Architecture for Authorization and Delegation in Distributed Object-Oriented Agent Systems*, Ph.D. Dissertation, Helsinki University of Technology, March 1999.

Other references

14. Sasu Tarkoma and Jaakko Kangasharju. Optimizing Content-based Routers: Posets and Forests. Distributed Computing 19 (1), September 2006.
15. Sasu Tarkoma and Jaakko Kangasharju. On the Cost and Safety of Handoffs in Content-based Routing Systems. Elsevier Computer Networks Journal. 2006 (in press). Available at: http://dx.doi.org/10.1016/j.comnet.2006.07.016